HP 1/8 G2 and MSL Encryption Kit User Guide

Abstract

This guide provides information about developing encryption key management processes, configuring the tape autoloader or tape library to implement the security policy based on the encryption kit, using and administering the autoloader or library with the encryption kit, and troubleshooting problems with the autoloader or library when using the encryption kit. This guide is intended for system administrators with knowledge of autoloader or library administration and operation, and security policies and procedures.

HP Part Number: AM495-96034
Published: June 2014
Edition: 5

© Copyright 2010, 2014 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel, Itanium, Pentium, Intel Inside, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows XP, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Contents

1 Features and overview....5
Considerations for using the encryption kit....5
LTO-4 and later generation tape drives and encryption....6
Requirements for using the encryption kit....6
Autoloader or library firmware requirements....7
Tape drive and drive firmware requirements....7
Access to the USB port....8
The key server token LED....8
The keys on the key server token....9
The token data backup and restore processes....11
Scenario 1....12
Scenario 2....12
Scenario 3....12
2 Creating your key management processes....14
When to create a new encryption key....14
Enabling automatic generation of new keys....14
Backing up the key server token data....14
Managing the token password (PIN)....16
Naming key server tokens....16
Maintaining encryption capability in the event of a power loss....17
3 Installing and configuring the encryption kit....18
Identifying product components....18
Preparing the autoloader or library....18
Log in to the remote management interface....18
Verify your autoloader or library firmware version....18
Locate the USB port....19
Preparing the key server tokens....19
Configuring encryption for the MSL6480....20
Insert the key server token....21
Enter the PIN....21
Configure the encryption mode and features....21
Backing up the initial key....28
Optional: Change the security user password....25
Configuring encryption for the autoloader and other libraries....25
Insert the key server token....25
Enter the PIN....26
Configure the encryption mode and features....26
Backing up the initial key....28
4 Using the encryption kit....30
Entering the PIN....30
After a power cycle....31
Changing the PIN....31
Generating a new encryption key....32
Enabling or disabling encryption....33
Backing up the token data....34
Restoring the token data....36
Restoring encrypted data....38
Combining keys from multiple key server tokens....39
When to obtain a new key server token....40
Seeding the new key server token....40

Restoring encrypted data during disaster recovery....41
Using the encryption kit with partitions or logical libraries....41
Restoring the encryption configuration after a chassis or library controller replacement....41
5 Troubleshooting....43
Installation problems....43
The library does not have a USB port....43
Operation problems....43
Encryption token LED....43
Troubleshooting table....44
MSL6480 event codes....46
Autoloader and other library event codes....47
6 Support and other resources....49
Contacting HP....49
Before you contact HP....49
HP contact information....49
Subscription service....49
Documentation feedback....49
Related information....49
Documents....49
Websites....49
Document conventions and symbols....50
Customer self repair....50
Index....51

1 Features and overview

IMPORTANT: The encryption kit provides secure encryption of your data using key server tokens and passwords. A thorough understanding and proper use of the encryption kit operation will maintain the security of your data and ensure that only qualified persons have access to the data. Managing your key server tokens and passwords is critical for preventing unauthorized data access and for avoiding the inability of qualified personnel to access data from tapes. Read and understand this encryption kit user guide before enabling encryption.

The encryption kit provides secure generation and storage of encryption keys. The encryption kit may be used with any HP StoreEver 1/8 G2 Tape Autoloader or the MSL2024, MSL4048, MSL6480, MSL8048 and MSL8096 Tape Library with at least one LTO-4 or later generation tape drive. The encryption kit is incompatible with the MSL6000.

The encryption kit includes two USB key server tokens. One key server token is available for use as a backup for the other.

To use the encryption kit, a key server token is inserted in the USB port on the back of the used with an autoloader or library, and encryption is enabled and configured from the remote management interface (RMI).

The encryption kit supports your manual security policies and procedures by providing secure storage for encryption keys. Access to the key server tokens and their backup files is protected with user-specified passwords. You will need to create processes to protect the tokens and secure the passwords.

The encryption kit requires support from the autoloader or library firmware and the tape drive firmware. See "Autoloader or library firmware requirements" (page 7) and "Tape drive and drive firmware requirements" (page 7). You can download autoloader or library firmware files from the HP Support website at http://www.hp.com/support.

IMPORTANT: When encryption is enabled with the encryption kit, the autoloader or library will not use encryption keys from other sources, such as a key management system or application software. Disable encryption in applications writing to the autoloader or library when encryption is enabled with the encryption kit. Applications that attempt to control encryption while encryption is enabled with the encryption kit will not be able to do so, which can cause backups or other write operations to fail.

Considerations for using the encryption kit

The purpose of encryption is to protect data from unauthorized access and use. For LTO-4 and later generation tape drives, the encryption algorithm is based on encryption keys. With the encryption kit, the encryption keys are stored on the key server token and access to the keys is protected by a password.

To enable, disable, and configure encryption on the MSL6480 library, you must be logged into the library RMI as the security user. For the autoloader or other libraries, you must be logged into the autoloader or library RMI using the administrator password.

To write encrypted data, you must have the key server token and the password for the key server token. Only one encryption key is used on a tape cartridge. If the tape cartridge contains previously-encrypted data, a key server token with the key for the tape must be in the autoloader or library.

To read encrypted data, you must have a key server token with the key for the tape and the password for the key server token. The association between the encryption key and the tape is not stored on either the key server token or the tape.

△ **CAUTION:** If you lose the key server tokens and token backup files associated with a tape, neither you nor HP will be able to recover the encryption keys that were stored on the tokens. HP recommends that a backup of the encryption keys be stored off site in a secure location.

If you lose the password to the key server token, neither you nor HP will be able to recover or reset the password to access the encryption keys. Without the password you will not be able to recover the data from tapes using the encryption keys on the token. HP recommends that you keep the password in a secure location, and that at least one copy of the password be kept off site in a secure location.

If the key server token is removed or becomes dislodged from the USB port on the back of the autoloader or library, the tape drive will not be able to read or write encrypted data. This could cause your backup or other data operation to fail.

Reading encrypted data from a tape cartridge requires the tape cartridge, a key server token with the encryption key for the tape, the password for the key server token, and the security password for the MSL6480 library or the administrator password for the autoloader or libraries. To prevent unauthorized access to your data, HP recommends keeping these items in safe and secure locations.

LTO-4 and later generation tape drives and encryption

The LTO-4 and later generation tape drives include hardware capable of encrypting data while writing data, and decrypting data when reading. Hardware encryption can be used with or without compression while maintaining the full speed and capacity of the tape drive and media.

NOTE: An LTO-4 or later generation tape drive will not write encrypted data to an LTO-3 or earlier generation tape. For additional compatibility information, see Media compatibility (page 7).

Encryption is the process of changing data into a form that cannot be read until it is deciphered with key used to encrypt the data, protecting the data from unauthorized access and use. LTO-4 and later generation tape drives use the 256-bit version of the industry-standard AES encrypting algorithm to protect your data.

Your company policy will determine when and how to use encryption. For example, encryption may be mandatory for company confidential and financial data, but not for personal data. Company policy will also define how encryption keys should be generated and managed, how frequently they should be changed, and how passwords are managed.

Encryption is primarily designed to protect the media once it is offline and to prevent it from being accessed by unauthorized users. You will be able to read and append the encrypted media as long as a key server token containing the correct key is installed and the appropriate passwords are available.

For more information about AES encryption, encryption keys, and using hardware encryption with your HP Ultrium tape drive, see the White Papers at http://h18006.www1.hp.com/storage/tapewhitepapers.html.

NOTE: Some earlier LTO-4 tape drive firmware revisions might not support the encryption kit functionality. Before enabling encryption, verify that the tape drive has firmware that supports the encryption kit. See "Tape drive and drive firmware requirements" (page 7) and update the firmware if necessary.

Requirements for using the encryption kit

Using the encryption kit requires support from the autoloader or library firmware and the tape drive firmware, as well as access to the USB port on the back of the autoloader or library.

Autoloader or library firmware requirements

MSL6480

All versions of MSL6480 library firmware support the encryption kit.

Autoloader and other libraries

To see whether your autoloader or library firmware supports the encryption kit, log into the RMI for your product. If the RMI has a **Status > Security** tab, the firmware supports the encryption kit.

Figure 1 Autoloader and other libraries Configuration > Security tab

If your autoloader or library does not have the **Status > Security** tab, you must download and install the current autoloader or library firmware. You can download autoloader or library firmware files from the HP Support website at http://www.hp.com/support.

Tape drive and drive firmware requirements

The autoloader or library must have at least one LTO-4 or later generation tape drive. Earlier generation tape drives do not support native encryption and cannot be used to encrypt or decrypt data with the encryption kit. When encryption is enabled, only LTO-4 tapes can be written in LTO-4 tape drives.

Table 1 Media compatibility

	LTO-4 drive	LTO-5 drive	LTO-6 drive
LTO-1 media	Incompatible	Incompatible	Incompatible
LTO-2 media	Read only	Incompatible	Incompatible
LTO-3 media	Read/Write (no encryption)	Read only	Incompatible
LTO-4 media — unencrypted	Read/Write	Read/Write	Read only
LTO-4 media — encrypted	Read/Write with encryption key	Read/Write with encryption key	Read only with encryption key
LTO-5 media — unencrypted	Incompatible	Read/Write	Read/Write
LTO-5 media — encrypted	Incompatible	Read/Write with encryption key	Read/Write with encryption key
LTO-5 media — unencrypted	Incompatible	Read/Write	Read/Write
LTO-5 media — encrypted	Incompatible	Read/Write with encryption key	Read/Write with encryption key
LTO-6 media — unencrypted	Incompatible	Incompatible	Read/Write
LTO-6 media — encrypted	Incompatible	Incompatible	Read/Write with encryption key

NOTE: Verify that the tape drive has the correct firmware before enabling encryption. All LTO-5 and later generation tape drives have firmware that supports the encryption kit. If you enable encryption with earlier versions of LTO-4 tape drive firmware, the autoloader or library will disable the tape drive port.

The LTO-4 tape drive must have the following or later versions of tape drive firmware:

	Parallel SCSI	SAS	Fibre Channel
Ultrium 1760	W22W	U26W	Not Applicable
Ultrium 1840	B45W	Not Applicable	H44W

To find the version of firmware on your tape drive, see "Verify your autoloader or library firmware version" (page 18).

NOTE: With the above LTO-4 tape drive firmware revisions, the autoloader or library will NOT allow LTO-3 media in LTO-4 tape drives when encryption is enabled with the encryption kit. Always ensure that your tape drive has the most recent firmware version. You can download tape drive firmware files from the HP Support website at http://www.hp.com/support.

Access to the USB port

To use the key server tokens included in the encryption kit, the USB port on the back of the autoloader or library must be accessible. Only the rear USB port on the MSL6480 may be used for the key server token. On some MSL2024 and MSL4048 libraries you might need to remove the silver tape covering the USB port.

Figure 2 MSL6480 rear USB port location

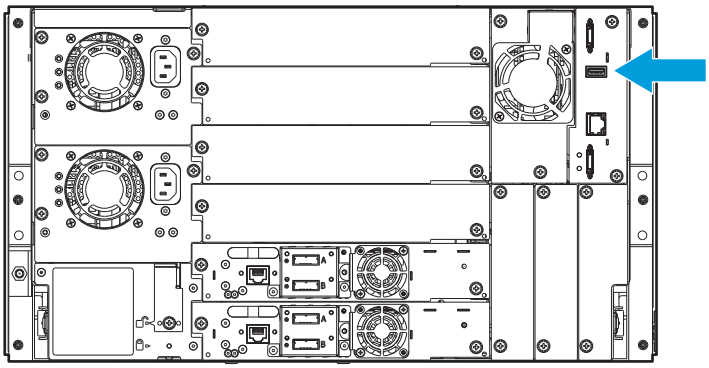
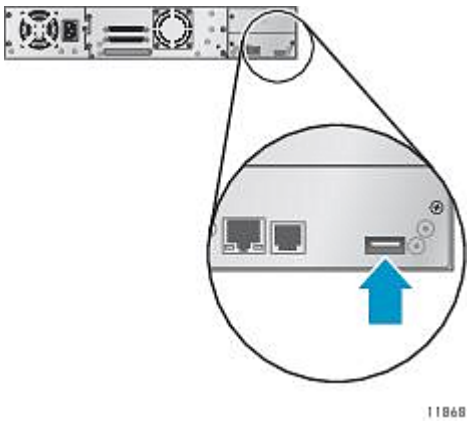


Figure 3 Autoloader and other library USB port location



The key server token LED

The key server token has a green status LED, which is visible through the token label.

Figure 4 Key server token LED

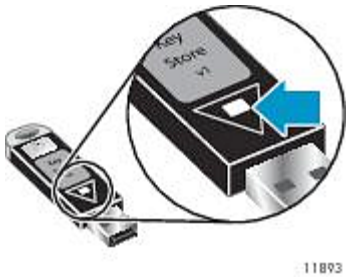


Table 2 Token status

LED behavior	Token status
On	The token is ready to be used by the autoloader or library.
Off	The token is not receiving power and must be fully inserted into the autoloader or library USB port.
Flashing	The device with the USB port does not have software to communicate with the key server token. If this occurs when the key server token is plugged into the autoloader or library, update the autoloader or library firmware to the current version. See "Encryption token LED" (page 43) for additional information about the key server token LED.

NOTE: The key server token is not a USB flash drive and its contents cannot be read by devices other than the autoloader or library.

The keys on the key server token

The encryption kit key server token generates, stores, and retrieves keys used both to encrypt data and to decrypt data. The same key is used as both the encryption key and the decryption key for a tape, but different tapes may use different keys.

Only one key is used at a time for encrypting data on new or formatted tapes in the autoloader or library. This key is called the *current key*. In most cases, the current key is the most recently created key. You can see the current key and key creation dates in the RMI **Status > Security** screen. On the MSL6480, click **Gather Key Information** to see the keys on the token.

When you manually create a new key or when the automatic key generation policy creates a new key, the previous current key will no longer be used to encrypt new or formatted tapes. All of the keys on the token, including the current key, are always available for decryption.

Figure 5 MSL6480 Status > Security screen showing the keys on the token and their dates of creation

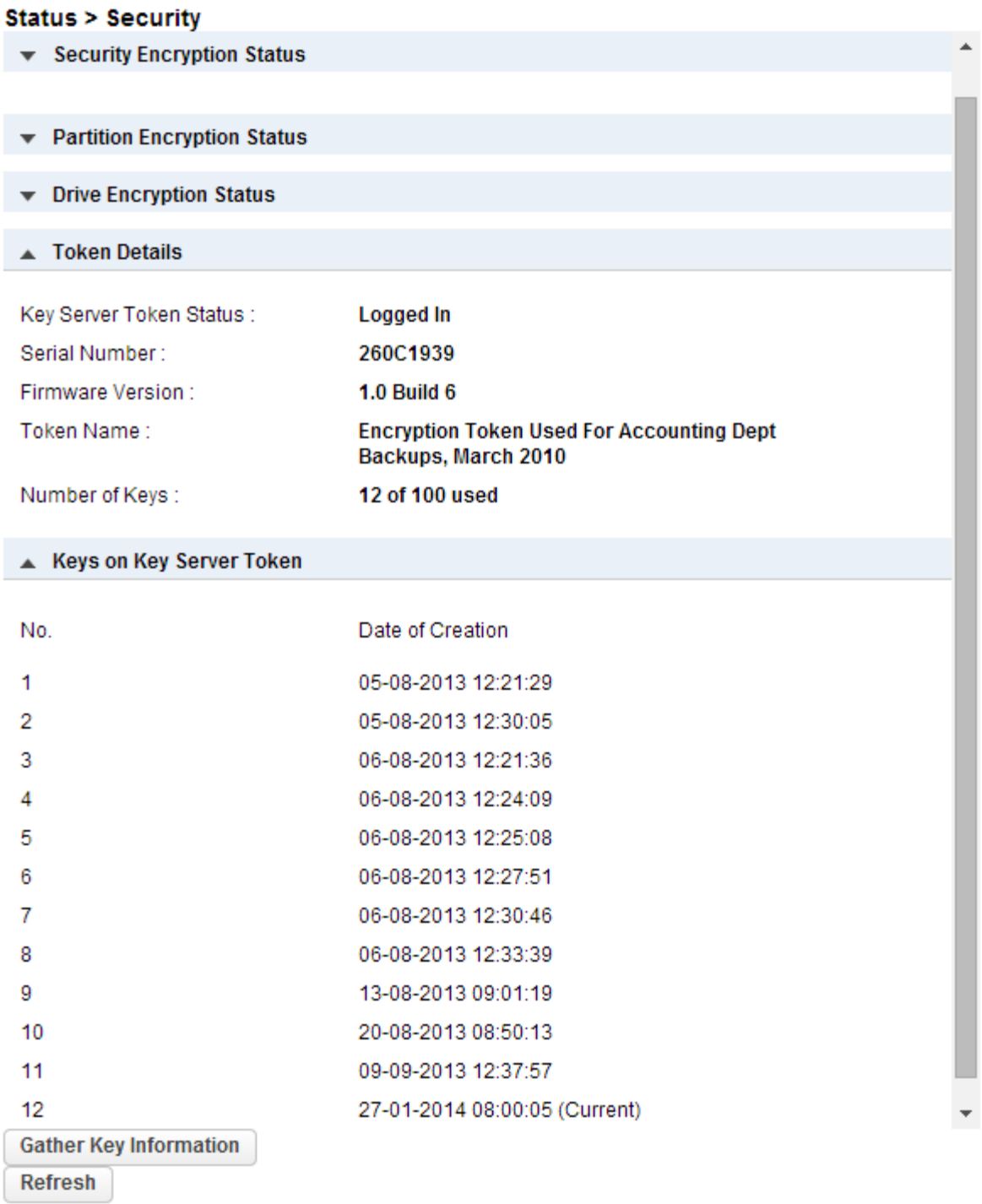
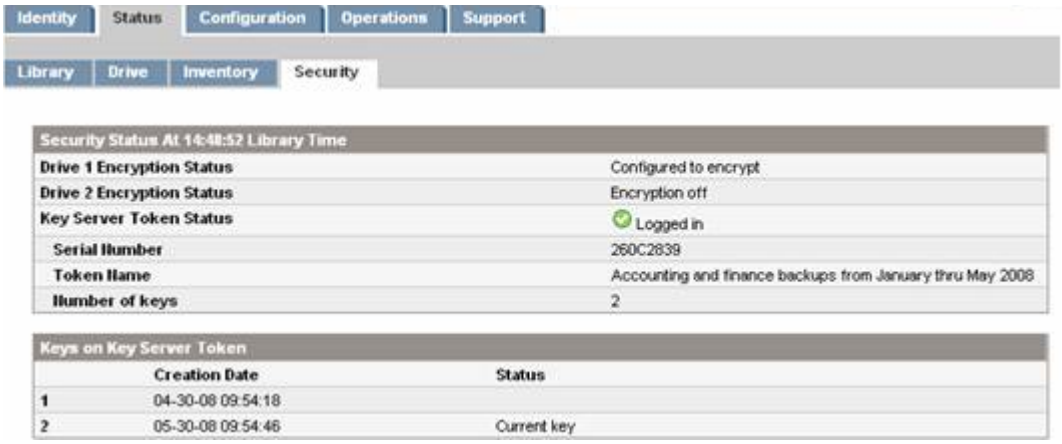


Figure 6 Autoloader and other libraries RMI Status > Security screen showing the Current key and key creation dates



The token can hold up to 100 keys. Any tape that was written using one of the keys on the token can be read using that token.

If an attempt is made to read an encrypted tape and the key is not on the installed token, an error message will be displayed when the tape drive attempts to read the tape. If your application supports appending data to a previously written tape, the original key used to write the tape must be available on the installed token to append data to the tape. Only one key is used to encrypt all of the data on a tape.

The status of each individual key in the **Keys on Key Server Token** section might inform you that a key has not had a backup operation performed on it. When you start the process to back up the token contents to a file, this status will be cleared. Also note that the backup status of the token might appear in the **Key Server Token Status** line in the upper portion of the screen. This status means that a backup is required, even if no individual keys in the **Keys on Key Server Token** section have this status. This situation usually occurs when a token has keys restored to it that were not on the original token. In this case, the autoloader or library has information that there are keys that have not been backed up, but cannot uniquely identify them. Always create a backup of the token whenever the **Key Server Token Status** indicates a backup is required.

The token data backup and restore processes

The encryption kit includes a process to back up the key server token data to a password-protected file and a process to restore the token backup file to a token. After the restore process, the receiving token contains a copy of each key from the backup file along with the keys it had before restore process. The receiving token will keep the same current key for writing encrypted tapes.

NOTE: After the second and subsequent restore operations to a token, the two tokens will never have the same current write key. If you need two tokens with the same write key, restore a backup of one token onto a new token.

In the following example, consider the tokens named Blue, Yellow, and Green:

The Blue token has current key D, with decryption keys A, B, C, and D.

Blue token
D = current key
C
B
A

The Yellow token has been initialized with a name “Yellow” but does not have any keys.

Yellow token

The Green token has current key F, with decryption keys F, A, and E. Key A is the same key A on the Blue token from a previous save/restore operation.

Green token
F = current key
E
A

Scenario 1

In this scenario, a backup file from the Blue token is restored to the Yellow token. Because the Yellow token does not have any keys, after the restore operation the Yellow token has all of the keys from the Blue token, with D as the current key.

Restoring to a token without keys is the only way for two tokens to have the same current key.

Yellow token (after restore)
D = current key
C
B
A

Scenario 2

In this scenario, a backup file from the Blue token is restored to the Green token. After the restore operation, the Green token contains all of the keys from both tokens. It only has one key A, which was on both tokens. It retains F as its current key.

Any tapes written with the Green token after the restore will be encrypted with a different key (F) than tapes written with the Blue token installed (D).

Green token (after restore)
F = current key
E
D
C
B
A

Scenario 3

In this scenario, a backup file from the Green token (after the restore in Scenario 2) is restored to the Blue token. After the restore operation, the both tokens have an identical set of keys, but do not have the same current key used to encrypt new and formatted tapes. The only way to create

two tokens with the same current key is to restore a backup onto a token that does not have any keys, as in Scenario 1.

Blue token (after restore)
F
E
D = current key
C
B
A

2 Creating your key management processes

The encryption kit provides encryption key generation and secure storage of the keys, and is intended to be used within a key management process. Processes should be developed to manage your encryption keys, tokens, and passwords before configuring encryption on the autoloader or library.

The key management processes may be based on your company's security and audit policies. Following are recommendations if your company does not have security policies or the security policies do not address areas needed for the key management processes. If you have highly sensitive data or are unsure about using encryption, HP recommends that you consult with a security expert to develop policies appropriate to your situation.

When to create a new encryption key

HP recommends that a new encryption key be created at least annually and at most weekly when using the encryption kit. The token can hold up to 100 keys. Once the key server token is full, additional key server tokens must be purchased. Keys can never be deleted from a key server token.

Your organization's backup and audit policies may specify when and how often to create a new key. If your organization's policies do not address creating new keys but include a frequency for replacing or archiving tapes, that policy could be basis for determining when and how often to create a new key.

NOTE: When initializing a token, you must create the first key manually. See "Generating a new encryption key" (page 32).

Enabling automatic generation of new keys

You can enable the autoloader or library to periodically generate a new encryption key and specify the number of weeks to use each key, as well as the day and time for generating new keys.

If you advance the autoloader or library time past a time when a new key would have been generated, the new key will not be generated. For example, if the automatic key generation policy is to generate a new key on Monday mornings and on Sunday the autoloader or library time is updated to a time on Tuesday, a new key will not be generated. When advancing the autoloader or library time, check the automatic key generation policy and manually generate a new key if necessary.

If the autoloader or library is powered off during a time when the automatic key generation policy would have generated a new key, a new key will be generated when the autoloader or library is powered on and the PIN is entered. Only one new key is generated, even if the autoloader or library was powered off for a time when multiple keys would have been generated had the autoloader or library been left on.

NOTE: Automatic key generation will not occur if media is loaded in any drive. When using automatic key generation, ensure that media is unloaded from the drives when keys are generated.

Backing up the key server token data

HP recommends that you back up the key server token data after a new key is created and before the new key is used to write tapes. The key server token data can be backed up to a password-protected file from the RMI. The backup process will save all of the keys, but not the token name or PIN.

The encryption kit includes two key server tokens. One token is intended to be installed in the autoloader or library to encrypt and decrypt tapes. If the first token is lost or damaged, the second token can be used in its place. The second token can also be used to read tapes with encrypted

data at a different location. If the second token contains a backup of the first token's data, it should be stored in a secure location, such as a fireproof safe in a different building.

The token data backup file and the second token support several approaches to backing up the keys so that tapes can continue to be written and read if the first token is lost or destroyed. Choose an approach that best meets your organization's needs and capabilities.

Table 3 Example token data backup processes

Backup process	Restore process	Benefits	Requirements
Back up the token backup file and store the uninitialized second token in a secure location.	Retrieve the token backup file from your organization's file backup program and restore it onto the unused second token.	• Avoids having to retrieve physical media containing the token data from an off-site location to create a new token data backup. • The token in use does not need to be removed from the autoloader or library during the token data backup process. • The token backup file can be restored onto any token. • The second token does not need to be stored in a secure location. • By using a new token for the restore process, the second token will have the same current key to encrypt tapes as the original token.	• Highly-reliable file backup and restore processes that store backup data off site. **NOTE:** If your file backup process writes encrypted data to an autoloader or a library using the encryption kit, be sure to back up the token data file to a different removable media, as in the next case. If the first token is lost or damaged, you will need the token backup file to restore onto a token and you will not be able to restore the token backup file from the encrypted tape without a token with a key for the tape.
Back up the token data to removable media, such as a USB flash drive or CD, and store it in a secure location.	Retrieve the backup media and second token from the secure location and restore the token data onto the second token.	• The token in use does not need to be removed from the autoloader or library during the token backup process. • The token backup file can be restored onto any token. • The second token does not need to be stored in a secure location. • If your file backup process uses an autoloader or a library with the encryption kit, you will be able to restore the token backup file to a new token if the token in use is lost or damaged.	• New backup media must be created when a new key is generated. • Token data backup files on removable media must be stored in a secure location.
Back up the token data on the first token to the second token and keep the second token in a secure location.	Retrieve the second token from the secure location and insert into any supported autoloader or library.	• The second token may be used immediately. • The token is easy to store in a secure location.	• The second token must be retrieved from the secure location to back up new keys created on the installed token. • The second token must be retrieved from the secure location if the first token is lost or damaged. • You must understand that the second token may not have the same current key used to encrypt tapes.

Managing the token password (PIN)

The token password, called a PIN, protects access to the data on the key server token.

IMPORTANT: The PIN is required to write and restore encrypted data. Neither you nor HP can recover, restore, or reset the PIN if it is lost or forgotten.

The PIN is set and can be changed from the RMI. Setting the PIN the first time also requires the appropriate RMI password. Changing the PIN requires both the current PIN and the appropriate RMI password.

- MSL6480 — Log into the RMI as the security user, which requires the security password.
- Autoloader and other libraries — Log into the RMI as the administrator, which requires the administrator password.

You must enter the PIN when:

- The autoloader or library powers on, cycles power, or is rebooted.
- The first time a token is inserted since the autoloader was powered on.
- When a token is inserted after another is removed.

You must enter the PIN each time the autoloader or library cycles power, the first time a token is inserted since the autoloader or library was powered on, and when a token is inserted after another is removed. The PIN does not need to be entered again if a token is removed and replaced without inserting a different token.

HP recommends that you create PIN management policies to ensure that the PIN is stored in a secure location and that it is only available to authorized personnel. The PIN management policies should consider:

- Ensuring that the PIN can be accessed by authorized personnel when necessary, even if the security officer or administrator is unavailable.
- Ensuring that the PIN is not accessible by unauthorized personnel.
- Ensuring that the PIN is not lost, damaged, or destroyed.
- Enabling, disabling, and configuring encryption requires both the appropriate RMI password and the token PIN. For increased security, the RMI password and token PIN can be known by different people, requiring two people to make these critical changes.

Naming key server tokens

The name of the key server token can have up to 126 characters. This is enough space to use a descriptive name, which can be helpful in determining which token has the encryption key for a particular tape if the documentation mapping the tokens and tapes is lost. For example, the name could include dates when the token was used, or the facility or department whose tapes are encrypted with keys on the token.

You can see the name of the token currently in the autoloader or library in the RMI without the PIN or a password. For the MSL6480 the token name is displayed on the main screen. For the autoloader and other libraries you can see the token name on the RMI **Status > Security** screen.

You can modify the name of the token currently in the autoloader or library from the RMI.

- MSL6480 — Log into the RMI as the security user, navigate to the **Configuration > Encryption > USB — MSL Encryption Kit** screen, and then enter the PIN to modify the token name in the **Pin Management** section. You will need the security user password.
- Autoloader and other libraries — Log into the RMI as the administrator user, navigate to the **Configuration > Security** screen, and then enter the PIN to modify the token name. You will need the administrator user password.

Maintaining encryption capability in the event of a power loss

For increased security, the key server token's PIN is stored in volatile memory in the autoloader or library. Each time the autoloader or library cycles power the PIN must be entered. The autoloader or library will display a warning message on the OCP and RMI, and send periodic SNMP and email events, if those options are enabled, until the PIN is entered. The autoloader or library will not write encrypted data when encryption is enabled until the PIN is entered.

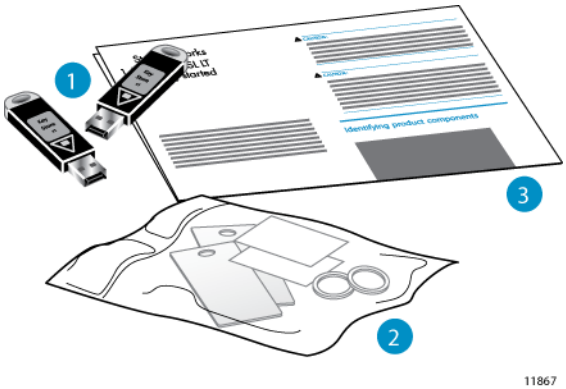
△ **CAUTION:** If it is critical that the autoloader or library maintain encryption capability in the event of a power loss, HP recommends that you plug the autoloader power cable or library power cable into an uninterruptible power supply.

3 Installing and configuring the encryption kit

Identifying product components

Verify that you received all of the product components.

Figure 7 Encryption kit components



1. Two key server tokens
2. Accessory bag of token id cards and holders
3. Product documentation

Preparing the autoloader or library

Log in to the remote management interface

The key server token and autoloader or library encryption capabilities can only be configured from the RMI.

- MSL6480 — Log into the RMI as the security user. You will need the security user password. The default password is `security`.
- Autoloader and other libraries — Log into the RMI as the administrator user. You will need the administrator user password.

If you have not used the RMI on this autoloader or library in the past, you may need to configure the network on the autoloader or library before continuing.

See the getting started guide or user guide for your autoloader or library for instructions on configuring the network and using the RMI. You can find these documents on the HP website at http://www.hp.com/support/manuals.

Verify your autoloader or library firmware version

All MSL6480 firmware versions support the encryption kit.

For the autoloader or other libraries, verify that your autoloader or library firmware version supports the encryption kit. If you see the **Status > Security** tab in the RMI, the firmware supports the encryption kit. If this tab is missing, update the autoloader or library firmware to the current version. Neither the administrator password nor token PIN are required to see the **Status > Security** tab.

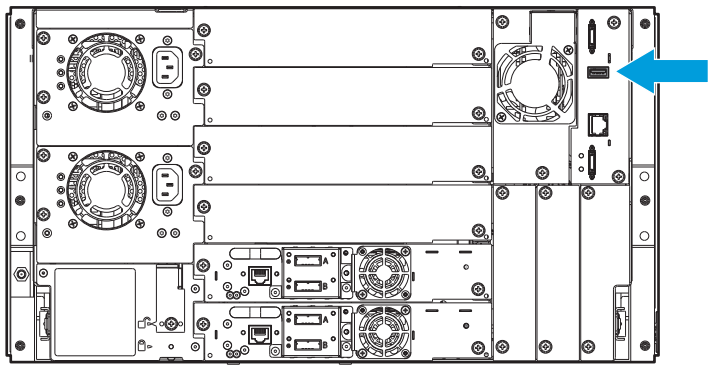
Figure 8 RMI Configuration > Security tab

You can download autoloader or library firmware files from the HP Support website at http >// www.hp.com/support.

Locate the USB port

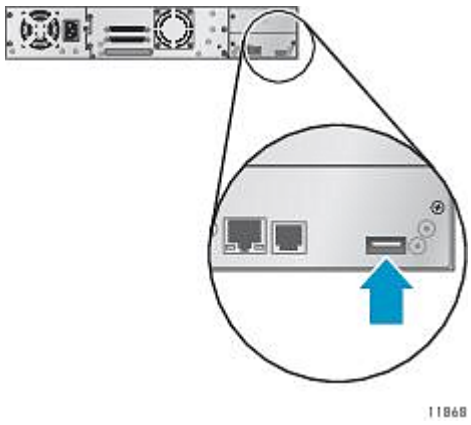
Locate the USB port on the back panel of the autoloader or library.

Figure 9 MSL6480 rear USB port location



NOTE: Only the rear USB port on the MSL6480 is used for the encryption kit token. The front port cannot be used for the token.

Figure 10 Autoloader and other library USB port location



If the USB port is covered with silver tape, remove the tape.

Preparing the key server tokens

As part of your security process, you will need to track each key server token, along with information associated with the token, as required by your security policy. If you do not have a security policy that specifies this information see "Creating your key management processes" (page 14) for

information about creating your encryption key management processes. HP recommends that you track at least:

- Token name
- Whether this token is a backup of another token
- Dates used for writing data
- The tape cartridges written with keys stored on the token. When possible, record the barcode label associated with the tape cartridge.
- Token backup file filename and password.

The encryption kit includes two methods of tracking the tokens. Choose the approach that works best for your security policy and organization. HP recommends that you use both approaches.

- Attached tag — The encryption kit includes a card and holder, which can be used to attach information to the token.
- Serial number — Each key server token has a unique serial number. You can use the serial number to identify the key server token and correlate the tape cartridges written with keys on the token.

TIP: The serial number is on the bottom of the token when the token is in the autoloader or library, making it difficult to see. You can also find the token serial number and firmware version on the RMI **Status > Security** screen.

IMPORTANT: HP recommends that you maintain a record of the tape cartridges that are written with encryption keys on the key server token. When restoring the data from an encrypted tape, you will need to use a key server token containing the encryption key for that tape. The name of the key server token is not stored on the tape and the name of the tape is not stored on the key server token. If you do not know which token contains the key for a tape, you may need to try all of your key server tokens when restoring data from an encrypted tape. Each key server token can contain a maximum of 100 keys.

NOTE: If you are using encryption kits with multiple autoloaders or libraries, you will need to track the autoloader or library used with each token as this information is not recorded on the token.

To use the attached tags to identify the tokens:

1. Write the token identification information on the paper cards.
2. Insert each card into a holder.
3. Attach the holders to the tokens.
4. Track the tape cartridges that are written with keys stored on the token and keep a copy of this record in a secure location.

To use the serial numbers to identify the tokens:

- Record the token identification information and tape cartridges that are written with keys stored on the token, and keep a copy of the record in a secure location.

TIP: The serial number is on the bottom of the token when the token is in the autoloader or library, making it difficult to see. You can find the token serial number and firmware version from the RMI.

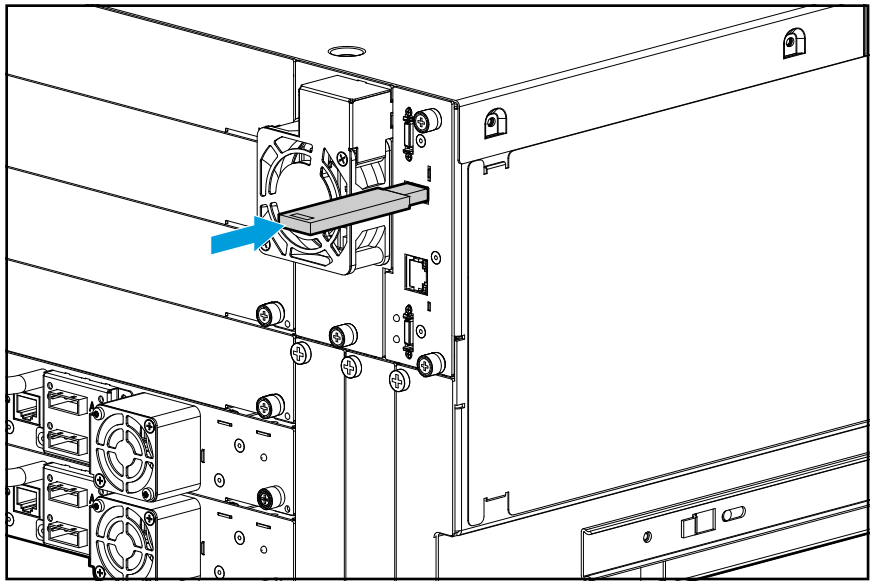
Configuring encryption for the MSL6480

In this section, you will configure the name and personal information number (PIN) for the key server token, and configure encryption for the MSL6480 library.

Insert the key server token

Insert the key server token in the USB port on the back panel of the library base module.

Figure 11 Inserting the key server token into the rear MSL6480 USB port



Enter the PIN

When a key server token is inserted for the first time in any autoloader or library, the autoloader or library will recognize it as a new token and display a dialog on the RMI requesting that you enter a PIN. The new PIN must be between eight and 16 characters long and contain at least one capitol letter, at least one lower case letter, and at least two digits. Follow the directions in the dialog to enter your PIN.

Store a copy of the PIN in a secure location.

△ **CAUTION:** The key server token protects the encryption keys with a PIN. If you lose the PIN, you will not be able to restore data from your encrypted tapes using that token. Neither you nor HP can recover a lost PIN. Keep a copy of the PIN in a safe place.

Configure the encryption mode and features

From the **Configuration > Encryption > USB — MSL Encryption Kit** screen you can enter the name of the token, save or restore token data to a file, or enable or disable encryption for the library. If your library is configured in multiple partitions, you can enable or disable encryption independently for each partition containing an LTO-4 or later generation tape drive. Only one encryption key is used at a time to write tape cartridges and the same encryption key is used by all tape drives in the library.

NOTE: If your application appends data to existing tapes, the key originally used to write the tape is used to append additional data to the tape; a key server token holding that key must be installed in the autoloader or library.

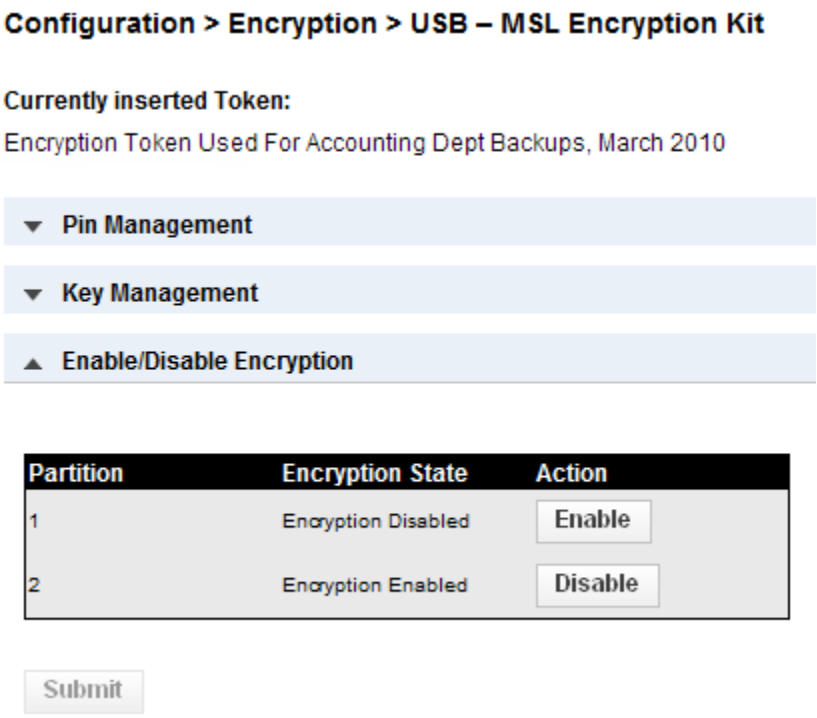
To configure the encryption mode and features:

1. Ensure that all tape drives are idle and do not contain media. The library will not change the encryption configuration if any drive in the library contains a tape.
2. Navigate to the **Configuration > Encryption** screen, select **USB — MSL Encryption Kit**, and then click **Submit**.

NOTE: This option is only selectable when a token is inserted in the rear USB port of the base module. Click **Refresh** to update the displayed key manager options.

3. Navigate to the **Configuration > Encryption > USB - MSL Encryption Kit** screen. If requested, enter the **Token PIN**, and then click **Submit**.
4. Click **Enable** in the **Enable/Disable Encryption** area to enable encryption for one or more partitions. Partitions that do not contain an LTO-4 or later generation tape drive will not appear on the configuration screen.

Figure 12 Enable/Disable Encryption area



5. Enter the name of the token in the **Token Name** field. The name can have up to 126 characters.

TIP: Using a descriptive name, including the dates when the keys on the token were used, could be helpful if your log of tapes written with keys on the token is lost.

6. Click **Submit** to apply your selections.
7. Generate the first key. By default, you must manually request the key server token to generate a new key. Click **Apply** in the **Key Management** area to generate the first key.

Figure 13 Key Management area

Configuration > Encryption > USB - MSL Encryption Kit
Currently inserted Token:
Encryption Token Used For Accounting Dept Backups, March 2010
PIN Management
Change PIN
Enter Current PIN
Enter New PIN
(The PIN must be at least 8 and max 16 characters long, contain at least one capital letter, one lower case letter and at least two digits. For more information about PIN formats and compatibility please read the Help page.)
Repeat new PIN:
Submit
Change Token name
New Token Name
Submit

8. Optional: Enable and configure automatic key generation. When automatic key generation is enabled, the library will automatically request the key server token to generate a new key periodically, according the policy you configure.
   a. Expand the **Key Management** section.
   b. Set the policy for the new key generation frequency, and the date and time this will occur. Be aware that when new keys are created automatically they are not backed up until you do so manually. To avoid only having one copy of the new key, set the automatic key generation policy for a time when you can back up the new key before tapes are written using the new key.
   c. Click **Submit** to apply your selections.

NOTE: A key is not generated when the library time is advanced past a time when a new key would have been generated. If you advance the library time, check the automatic key generation policy to see whether a new key is needed, and if so, manually generate it.

One new key is generated if the library is off at a time when a new key would have been automatically generated. To prevent a new key from being generated in this case, disable automatic key generation before powering off the library.

NOTE: Automatic key generation will not occur if media is loaded in any drive. When using automatic key generation, ensure that media is unloaded from the drives when keys are generated.

NOTE: The library uses the same write encryption key (the Current key) for all partitions with encryption enabled. If the library is writing an encrypted tape when you change the security configuration, the new configuration will take effect for the next tape loaded into an LTO-4 or later generation tape drive.

Backing up the initial key

The key server token contains the keys used to encrypt and decrypt your tapes. HP strongly recommends that you back up the keys on the token to allow you to access your data if a token is lost or damaged. When backing up the key server token data, the token data is saved to a password-protected file. You can then back up that file with a file backup process, archive it on other media, such as a USB flash drive or CD, and restore it to the second key server token. For more information about creating a process for backing up the key server token data, see "Backing up the key server token data" (page 14)

CAUTION: When a new key is created, HP recommends that you always back up the token data and store the backup in a safe place. You will not be able to restore data from your encrypted tapes without a token containing the encryption key used to write the tape and the token PIN. Neither you nor HP can recover the key used to write a tape without a token containing the key and the token PIN.

If the token data is saved to a file, you can create a token from the file at any time if you know the file password, even if the original token is not available.

To back up the information on the key server token to a file:

1. Verify that the token to be backed up is in the USB port on the back of the autoloader or library.
2. Navigate to the **Configuration > Encryption > USB — MSL Encryption Kit** screen **Key Management** area.
3. Enter a new password to be used to protect access to the contents of the backup file in the **Enter Token Backup File Password** and **Repeat Token Backup File Password** fields. For increased security, do not use the token PIN.

   The backup file password must be between eight and 16 characters, containing at least one capital letter, one lower case letter, and at least two digits.

   NOTE: Some firmware versions limit the backup file password to 15 characters. For optimal interoperability, limit the length of the backup file password to 15 characters.

4. Click **Save** and follow the instructions as they appear on the screen to specify a location for the token backup file.

   NOTE: If your browser has a pop-up blocker enabled, the file dialog box may not appear. Turn off your pop-up blocker before clicking **Save**.

5. Save the token backup file to removable media or a location where it will be backed up by your file backup process, if applicable. Store the removable media with the token backup file in a secure location.

   NOTE: If your file backup process backs up encrypted files to an autoloader or a library using the encryption kit, keep another copy of the file on removable media, such as a USB flash drive or CD, or on the second token. If the first token is lost or damaged you will not be able to restore the token backup file from an encrypted tape to create a replacement token.

If your token data backup policy is to back up the token data on the second token, to do so:

1. Insert the second token into the USB port on the back of the autoloader or library.
2. Set the PIN and token name, as you did for the first token.

3. Navigate to the **Configuration > Encryption > USB — MSL Encryption Kit** screen.
4. In the **Restore Token Backup from File** pane, enter the Token Restore File Password. (The Token Restore File Password is the Token Backup File Password used when the token backup file was created.)
5. Click **Submit Token Restore File Password**.
6. Enter the location of the token backup file. (The **Browse** button will be active after the token restore file password is submitted.)

   NOTE: Each key server token can hold up to a maximum of 100 keys. If the token backup file and the token receiving the restore contain over 100 unique keys, the restore process will not be initiated. You will receive warnings when the key server token is over 90% full. You should purchase new tokens and transition to using a new token when these warnings appear. Keys can never be deleted from the key server token.

7. Click **Restore**.
8. After the backup process is complete, return the first key server token to the rear USB port of the library.
9. Store the second key server token in a secure location.

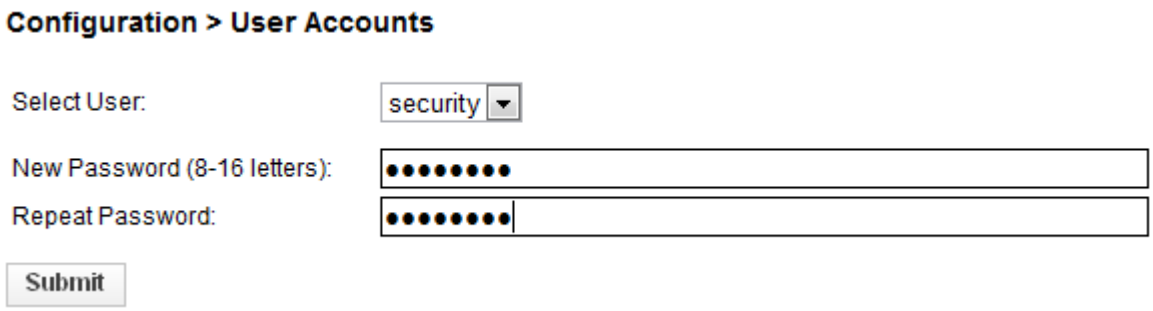
CAUTION: The token must be in the USB port of the library to read or write encrypted data. If the token is dislodged or removed, your backups could fail. If the token is lost, you will not be able to restore the data from your encrypted tapes unless you have a token with the keys used to write the tapes.

Optional: Change the security user password

The library is shipped with a default password for the security user. For increased security, change the password for the security user.

From the **Configuration > User Accounts** screen, select the security user, enter the new password twice, and then click **Submit**. The password must contain eight to 16 characters, which can include upper and lower case letters, numbers, and special characters.

Figure 14 Changing the security user password in the Configuration > User Accounts screen



Configuring encryption for the autoloader and other libraries

In this section, you will configure the name and personal information number (PIN) for the key server token, and configure encryption on the autoloader or library.

Insert the key server token

Insert the key server token in the USB port on the back panel of the autoloader or library.

Figure 15 Inserting the key server token

Enter the PIN

When a key server token is inserted for the first time in any autoloader or library, the autoloader or library will recognize it as a new token and display a dialog on the RMI requesting that you enter a PIN. The new PIN must be between eight and 16 characters long and contain at least one capitol letter, at least one lower case letter, and at least two digits. Follow the directions in the dialog to enter your PIN.

NOTE: Some older versions of autoloader and MSL2024, MSL4048, and MSL8096 library firmware versions limit the PIN length to 15 characters. For optimal interoperability limit the length of the PIN to 15 characters or ensure that the most current firmware is installed on your devices.

Store a copy of the PIN in a secure location.

△ **CAUTION:** The key server token protects the encryption keys with a PIN. If you lose the PIN, you will not be able to restore data from your encrypted tapes using that token. Neither you nor HP can recover a lost PIN. Keep a copy of the PIN in a safe place.

Configure the encryption mode and features

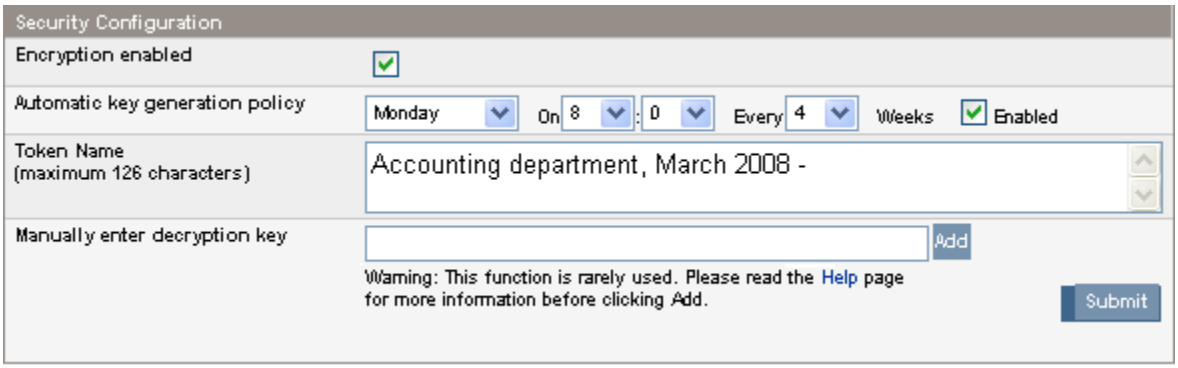
From the **Configuration > Security** screen you can enter the name of the token, enable or disable encryption for the autoloader or library, and enable the autoloader or library to automatically generate a new key. If your library is configured in multiple logical libraries, you can enable or disable encryption independently for each logical library containing an LTO-4 or later generation tape drive. Only one encryption key is used at a time to write tape cartridges and the same encryption key is used by all tape drives in the library.

NOTE: If your application appends data to existing tapes, the key originally used to write the tape is used to append additional data to the tape; a key server token holding that key must be installed in the autoloader or library.

To configure the encryption mode and features:

1. Click the **Encryption enabled** box to enable encryption for the autoloader or library, or for one or more logical libraries that contain an LTO-4 or later generation tape drive. Logical libraries that do not contain an LTO-4 or later generation tape drive will not appear on the configuration screen.

Figure 16 Security Configuration pane of the Configuration > Security screen



2. Enter the name of the token in the **Token Name** field. The name can have up to 126 characters.

TIP: Using a descriptive name, including the dates when the keys on the token were used, could be helpful if your log of tapes written with keys on the token is lost. This descriptive name will appear on the RMI whenever the token is installed. You do not need to enter the name for authentication.

3. Click **Submit** in the **Security Configuration** pane to apply your selections.
4. Generate the first key. By default, you must manually request the key server token to generate a new key. Click **Apply** in the **Generate a new write key** pane to generate the first key.

Figure 17 Generate a new write key pane of the Configuration > Security screen

5. Optional: Enable and configure automatic key generation. When automatic key generation is enabled, the autoloader or library will automatically request the key server token to generate a new key periodically, according the policy you configure. Set the policy for the new key generation frequency, and the day and time this will occur. Be aware that when new keys are created automatically they are not backed up until you do so manually. To avoid only having one copy of the new key, set the automatic key generation policy for a time when you can back up the new key before tapes are written using the new key.

   Click **Submit** in the **Security Configuration** pane to apply your selections.

NOTE: A key is not generated when the autoloader or library time is advanced past a time when a new key would have been generated. If you advance the autoloader or library time, check the automatic key generation policy to see whether a new key is needed, and if so, manually generate it.

One new key is generated if the autoloader or library is off at a time when a new key would have been automatically generated. To prevent a new key from being generated in this case, disable automatic key generation before powering off the autoloader or library.

NOTE: Automatic key generation will not occur if media is loaded in any drive. When using automatic key generation, ensure that media is unloaded from the drives when keys are generated.

NOTE: The autoloader or library uses the same write encryption key (the Current key) for all logical libraries with encryption enabled. If the autoloader or library is writing an encrypted tape when you change the security configuration, the new configuration will take effect for the next tape loaded into an LTO-4 or later generation tape drive.

Backing up the initial key

The key server token contains the keys used to encrypt and decrypt your tapes. HP strongly recommends that you back up the keys on the token to allow you to access your data if a token is lost or damaged. When backing up the key server token data, the token data is saved to a password-protected file. You can then back up that file with a file backup process, archive it on other media, such as a USB flash drive or CD, and restore it to the second key server token. For more information about creating a process for backing up the key server token data, see "Backing up the key server token data" (page 14)

△ **CAUTION:** When a new key is created, HP recommends that you always back up the token data and store the backup in a safe place. You will not be able to restore data from your encrypted tapes without a token containing the encryption key used to write the tape and the token PIN. Neither you nor HP can recover the key used to write a tape without a token containing the key and the token PIN.

If the token data is saved to a file, you can create a token from the file at any time if you know the file password, even if the original token is not available.

To back up the information on the key server token to a file:

1. Verify that the token to be backed up is in the USB port on the back of the autoloader or library.
2. Navigate to the **Configuration > Security** screen **Back up Token to File** pane.
3. Enter a new password to be used to protect access to the contents of the backup file in the **Enter Token Backup File Password** and **Repeat Token Backup File Password** fields. For increased security, do not use the token PIN.

   The backup file password must be between eight and 16 characters, containing at least one capital letter, one lower case letter, and at least two digits.

   NOTE: Some firmware versions limit the backup file password to 15 characters. For optimal interoperability, limit the length of the backup file password to 15 characters.

4. Click **Submit Token Backup File Password**.
5. Click **Save** and follow the instructions as they appear on the screen to specify a location for the token backup file.

   NOTE: If your browser has a pop-up blocker enabled, the file dialog box may not appear. Turn off your pop-up blocker before clicking **Save**.

6. Save the token backup file to removable media or a location where it will be backed up by your file backup process, if applicable. Store the removable media with the token backup file in a secure location.

   NOTE: If your file backup process backs up encrypted files to an autoloader or a library using the encryption kit, keep another copy of the file on removable media, such as a USB flash drive or CD, or on the second token. If the first token is lost or damaged you will not be able to restore the token backup file from an encrypted tape to create a replacement token.

If your token data backup policy is to back up the token data on the second token, to do so:

1. Insert the second token into the USB port on the back of the autoloader or library.
2. Set the PIN and token name, as you did for the first token.

3. Navigate to the **Configuration > Security** screen.
4. In the **Restore Token Backup from File** pane, enter the Token Restore File Password. (The Token Restore File Password is the Token Backup File Password used when the token backup file was created.)
5. Click **Submit Token Restore File Password**.
6. Enter the location of the token backup file. (The **Browse** button will be active after the token restore file password is submitted.)

Figure 18 Restore Token from File pane of the Configuration > Security screen

NOTE: Each key server token can hold up to a maximum of 100 keys. If the token backup file and the token receiving the restore contain over 100 unique keys, the restore process will not be initiated. You will receive warnings when the key server token is over 90% full. You should purchase new tokens and transition to using a new token when these warnings appear. Keys can never be deleted from the key server token.

7. Click **Restore**.
8. After the backup process is complete, return the first key server token in the USB port of the autoloader or library.
9. Store the second key server token in a secure location.

CAUTION: The token must be in the USB port of the autoloader or library to read or write encrypted data. If the token is dislodged or removed, your backups could fail. If the token is lost, you will not be able to restore the data from your encrypted tapes unless you have a token with the keys used to write the tapes.

4 Using the encryption kit

You can access encryption kit features from the RMI. Accessing the RMI encryption kit configuration screen requires a password.

Table 4 RMI encryption kit configuration screen, user, and password

Device	RMI screen	User	Password
MSL6480	**Configuration > Encryption > USB – MSL Encryption Kit**	Security	Security user password
Autoloader and other libraries	**Configuration > Security**	Administrator	Administrator user password

NOTE: Some RMI options may not be available until the autoloader or library has completed its power on cycle. Buttons that are grayed out might become available when the power on cycle is completed.

Entering the PIN

The PIN is a password that protects access to the data on the key server token. When you insert a different key server token or power on the autoloader or library, you must enter the key server token password (PIN) from the RMI before the autoloader or library will read or write encrypted data using keys from the token.

Figure 19 MSL6480 — Entering the PIN in the encryption kit configuration screen

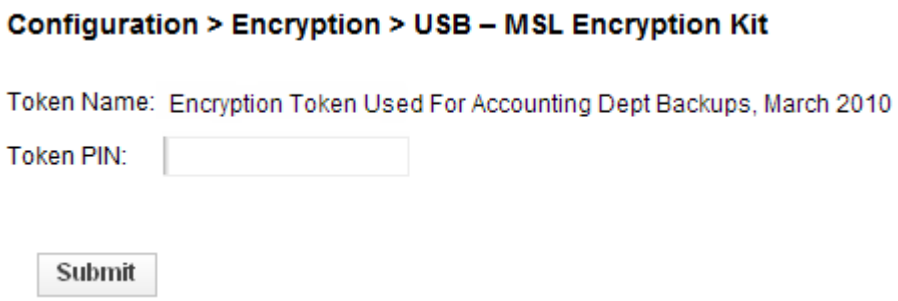
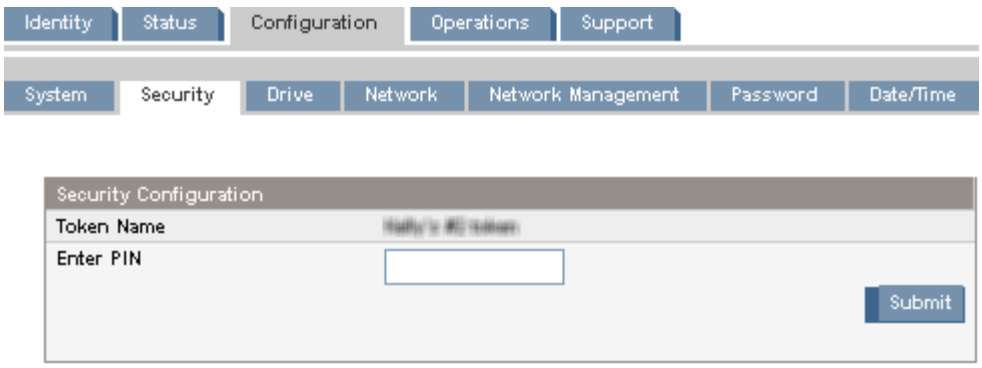

Configuration > Encryption > USB – MSL Encryption Kit
Token Name: Encryption Token Used For Accounting Dept Backups, March 2010
Token PIN:
Submit

Figure 20 Autoloader and other libraries — Entering the PIN in the encryption kit configuration screen



After entering the PIN you will be able to configure the encryption kit for the duration of the RMI session. The RMI session will end automatically after about five minutes without RMI user interaction. You can click **Logout** in the upper right corner of the RMI screen banner to end the RMI session immediately.

NOTE: After the RMI session ends, the PIN will still be available to the autoloader or library to access the keys on the token for writing and reading tapes. For encryption operation, the PIN only needs to be entered once when the autoloader or library is powered on or a different token is installed in the autoloader or library.

Figure 21 MSL6480 RMI Logout link

Figure 22 Autoloader and other library RMI Logout link

After a power cycle

For increased security, the key server token's PIN is stored in volatile memory in the autoloader or library. Each time the autoloader or library is powered on, the PIN must be entered. The autoloader or library will display a warning message on the OCP and RMI, and send periodic SNMP and email events, if those options are enabled, until the PIN is entered. The autoloader or library will not write encrypted data until the PIN is entered.

CAUTION: If it is critical that the autoloader or library maintain encryption capability in the event of a power loss, it is recommended that you plug the autoloader power cable or the library power cable into an uninterruptable power supply (UPS).

Changing the PIN

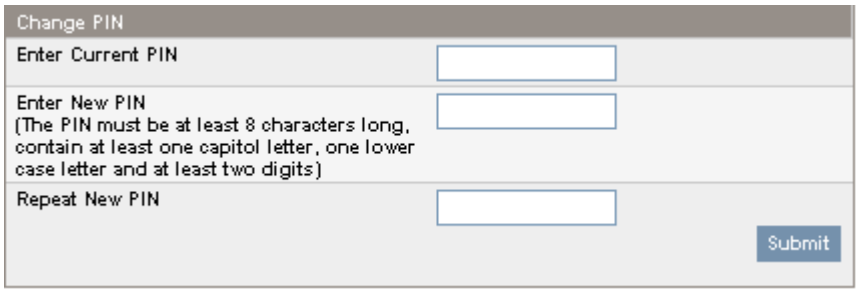
You can change the PIN from the RMI encryption kit configuration screen with the required password. The PIN must be between eight and 16 characters, containing at least one capital letter, one lower case letter, and at least two digits.

NOTE: Some firmware versions limit the PIN to 15 characters. For optimal interoperability, limit the length of the backup file password to 15 characters.

Figure 23 MSL6480 — Changing the PIN in the encryption kit configuration screen

Configuration > Encryption > USB - MSL Encryption Kit
Currently inserted Token:
Encryption Token Used For Accounting Dept Backups, March 2010
PIN Management
Change PIN
Enter Current PIN
Enter New PIN
(The PIN must be at least 8 and max 16 characters long, contain at least one capital letter, one lower case letter and at least two digits. For more information about PIN formats and compatibility please read the Help page.)
Repeat new PIN:
Submit
Change Token name
New Token Name
Submit

Figure 24 Autoloader and other libraries — Changing the PIN in the encryption kit configuration screen


Change PIN
Enter Current PIN
Enter New PIN
(The PIN must be at least 8 characters long, contain at least one capitol letter, one lower case letter and at least two digits)
Repeat New PIN
Submit

Generating a new encryption key

You can generate a new encryption key from the RMI encryption kit configuration screen with the required password.

Figure 25 MSL6480 — Generating a new encryption key in the encryption kit configuration screen

Configuration > Encryption > USB - MSL Encryption Kit
Currently inserted Token:
Encryption Token Used For Accounting Dept Backups, March 2010
PIN Management
Change PIN
Enter Current PIN
Enter New PIN
(The PIN must be at least 8 and max 16 characters long, contain at least one capital letter, one lower case letter and at least two digits. For more information about PIN formats and compatibility please read the Help page.)
Repeat new PIN:
Submit
Change Token name
New Token Name
Submit

To generate a new encryption key, click **Apply** in the **Key Management** pane. The library will take a few seconds to generate the new key.

Figure 26 Autoloader and other libraries — Generating a new encryption key in the encryption kit configuration screen

To generate a new encryption key, click **Apply** in the **Generate a new write key** pane. The autoloader or library will take a few seconds to generate the new key.

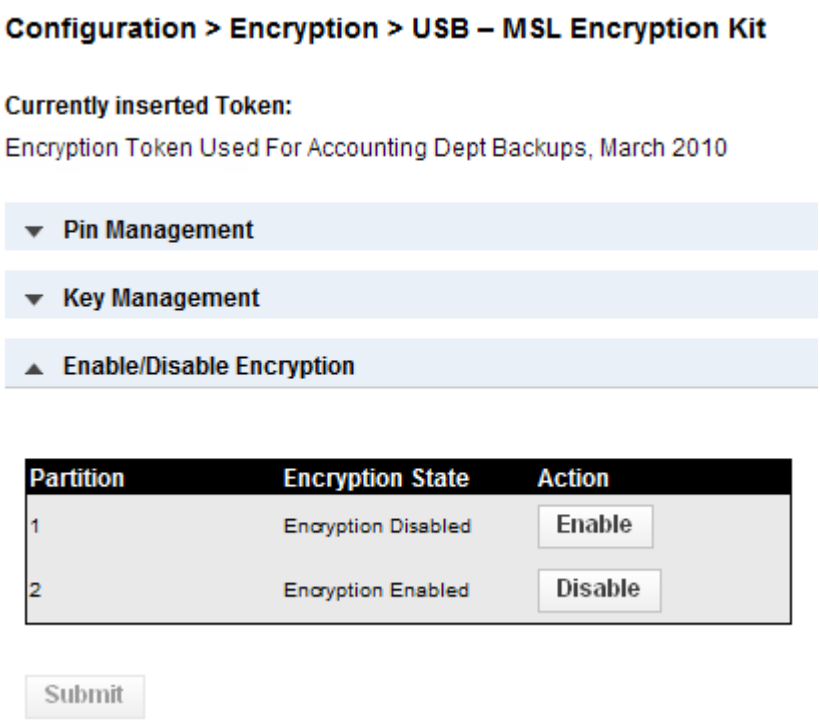
The new key will be used starting with the next new or formatted tape written. Only one key is used to write all of the data on a tape.

NOTE: The key server token holds a maximum of 100 keys.

Enabling or disabling encryption

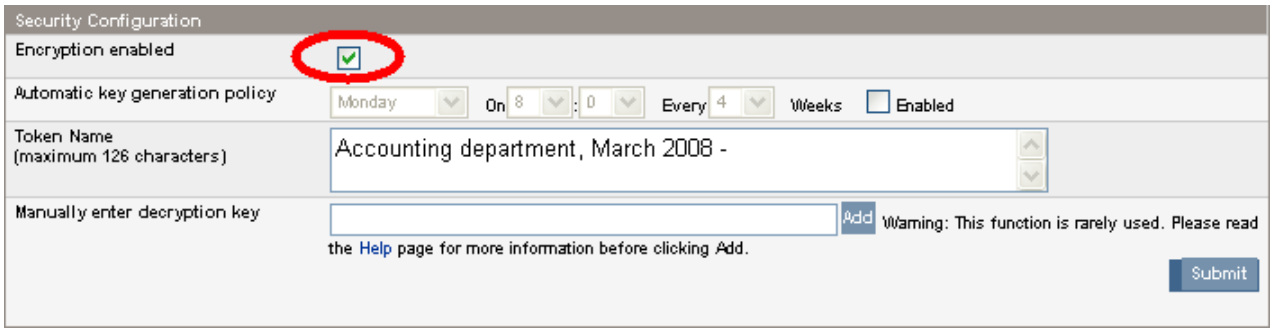
You can enable or disable encryption from the RMI encryption kit configuration screen with the required password.

Figure 27 MSL6480 — Enabling encryption in the encryption kit configuration screen



Click **Enable** to enable encryption for the partition. Click **Disable** to disable encryption for the partition.

Figure 28 Autoloader and other libraries — Enabling encryption in the encryption kit configuration screen



Click in the **Encryption enabled** box to enable or disable encryption. The green check mark shows that encryption is enabled.

Enabling encryption will enable encryption for all LTO-4 or later generation tape drives in the library.

Enabling or disabling encryption will take effect on the next tape unload for each tape drive. The encryption mode for a tape will not change while the tape is being written. Once a tape drive has started the decryption process for a tape, that tape's data will continue to be decrypted until the tape is unloaded.

Backing up the token data

You can back up the token data from the RMI encryption kit configuration screen with the required password.

Figure 29 MSL6480 — Backing up the token data from the encryption kit configuration screen

Configuration > Encryption > USB - MSL Encryption Kit
Currently inserted Token:
Encryption Token Used For Accounting Dept Backups, March 2010
PIN Management
Change PIN
Enter Current PIN
Enter New PIN
(The PIN must be at least 8 and max 16 characters long, contain at least one capital letter, one lower case letter and at least two digits. For more information about PIN formats and compatibility please read the Help page.)
Repeat new PIN:
Submit
Change Token name
New Token Name
Submit

Figure 30 Autoloader and other libraries — Backing up the token from the Back up Token to File pane of the encryption kit configuration screen

Back up Token to File
Enter Token Backup File Password
(The Token Backup File Password must be at least 8 characters long, contain at least one capital letter, one lower case letter and at least two digits)
Repeat Token Backup File Password
Submit Token Backup File Password
Back up Token to File
Save

During the token backup process, the autoloader or library will write the token information to a file, which will be saved on the computer from which you are running the browser with the RMI. After the file is written, the information can be restored to a different token.

During the restore process, the encryption keys from the file will be merged with the keys on the token. If the number of unique keys from the two sources is greater than 100, the restore process will not be initiated.

TIP: If you want two tokens to both have all of the keys, perform the backup and restore procedures twice, starting each time with a different token. Each token will retain its current key used to write new or formatted tapes, but both tokens can be used to decrypt tapes written with keys from either token.

To back up the information on a token to a file:

1. Log into the RMI encryption kit screen. To do so, you will need to log into the RMI and supply the PIN for the token in the autoloader or library.
   - MSL6480 — Log into the RMI as the security user and navigate to the **Configuration > Encryption > USB — MSL Encryption Kit** screen. You will need the security user password.
   - Autoloader and other libraries — Log into the RMI as the administrator user and navigate to the **Configuration > Security** screen. You will need the administrator user password.
2. In the **Back up Token to File** pane, enter a password, which will be used to secure the data file on the computer, in both fields. The second one ensures that the password was typed correctly.

   The backup file password must be between eight and 16 characters, containing at least one capital letter, one lower case letter, and at least two digits.

   NOTE: Some firmware versions limit the backup file password to 15 characters. For optimal interoperability, limit the length of the backup file password to 15 characters.
3. Autoloader and other libraries — Click **Submit Token Backup File Password**.
4. Click **Save**. The RMI will prompt you for the location to save the file. Follow the instructions in RMI.

Restoring the token data

You can restore the token data from the RMI encryption kit configuration screen with the required password.

Figure 31 MSL6480 — Restoring the token data from the Restore Token from File area of the encryption kit configuration screen

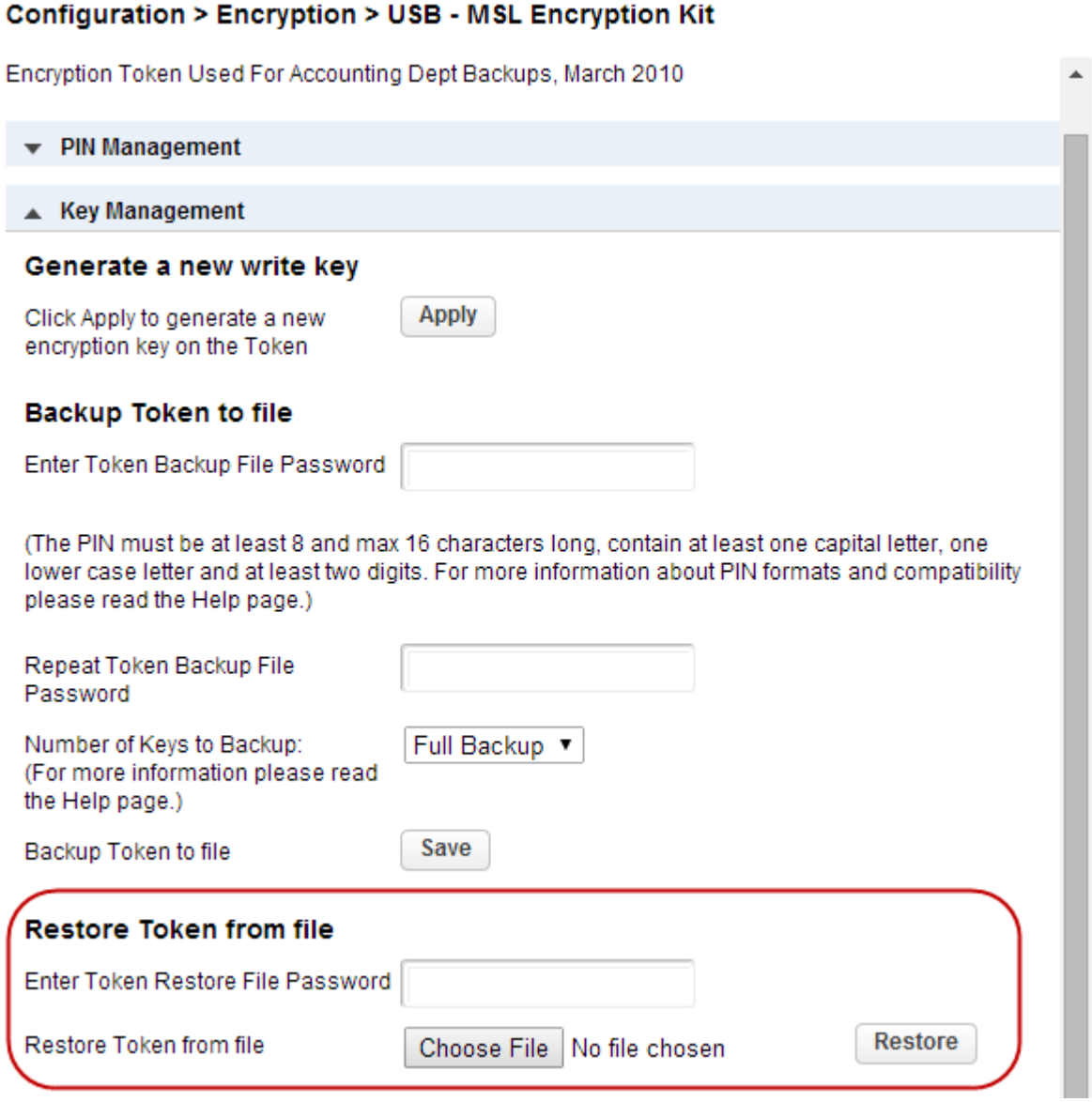

Configuration > Encryption > USB - MSL Encryption Kit
Encryption Token Used For Accounting Dept Backups, March 2010
PIN Management
Key Management
Generate a new write key
Click Apply to generate a new encryption key on the Token
Apply
Backup Token to file
Enter Token Backup File Password
(The PIN must be at least 8 and max 16 characters long, contain at least one capital letter, one lower case letter and at least two digits. For more information about PIN formats and compatibility please read the Help page.)
Repeat Token Backup File Password
Number of Keys to Backup:
(For more information please read the Help page.)
Full Backup
Backup Token to file
Save
Restore Token from file
Enter Token Restore File Password
Restore Token from file
Choose File
No file chosen
Restore

Figure 32 Autoloader and other libraries — restoring token data from the Restore Token from File pane of the encryption kit configuration screen

During the restore process, the encryption keys from the file will be merged with the keys on the token. If the number of unique keys from the two sources is greater than 100, the restore process will not be initiated. To ensure that all of the keys are on both tokens, perform the backup and restore procedures twice, starting each time with a different key.

The write key after the restore will be the one from the token receiving the restore, unless the token receiving the restore does not have any keys. For more information about backing up and restoring the token data, along with examples of how these operations affect the write key, see "The token data backup and restore processes" (page 11).

To restore a token backup file to a token:

1. If you are restoring the token backup file to a different token than the one installed in the autoloader or library, pause all write operations to LTO-4 or later generation tape drives with encryption enabled.
2. Log into the RMI.
   - MSL6480 — Log into the RMI as the security user. You will need the security user password.
   - Autoloader and other libraries — Log into the RMI as the administrator user. You will need the administrator user password.
3. Insert the token that will receive the data from the token backup file into the USB port of the autoloader or library if necessary.
4. Access the RMI encryption kit configuration screen for your device. Enter the PIN if requested. If this is a new token, follow the instructions on the RMI to create a PIN.
5. If this is a new token, enter the name in the **Token Name** field and click **Submit** in that pane.
6. Enter the password used to create the token backup file. Click **Submit Token Restore File Password**.

Figure 33 Restore Token from File pane of the RMI Configuration > Security screen

7. Browse to the location of the token backup file. Click **Restore**. (The Browse button will be active after the token restore file password is submitted.)

NOTE: The key server token holds up to 100 keys. If more than 100 unique keys are found on the receiving token and in the backup file, the restore process will not be initiated. You will receive warnings when a key server token is over 90% full. You should purchase new tokens and transition to using a new token when these warnings appear. Keys can never be deleted from a key server token.

8. Return the original token to the USB port of the autoloader or library if necessary.
9. If you paused write operations at the beginning of the procedure, you can resume them.

Restoring encrypted data

When you restore encrypted data from a tape cartridge, the autoloader or library will verify that the encryption key for the tape exists on the key server token installed in the USB port of the autoloader or library. If the token is not installed in the USB port of the autoloader or library, or the key is not found on the token, the OCP and RMI will display an error message.

The key server token containing the key for the tape to be restored must be installed in the autoloader or library USB port before the tape is read. You will need to enter the PIN for the token when the token is inserted into the autoloader or library.

A library with multiple LTO-4 or later generation tape drives will continue writing other tapes with the newest encryption key on the token installed in the library while restoring the encrypted data.

IMPORTANT: Pause all write operations when restoring data using a different token than the one used for writing new or formatted tapes. Not doing so can result in data written with an encryption key different than the one on the original token.

NOTE: If the token is removed while a tape drive is reading or writing a tape, the tape drive will continue reading or writing encrypted data until the tape is removed or the tape drive is reset.

Combining keys from multiple key server tokens

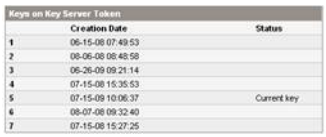
You may want to combine the encryption keys from two or more key servers to read tapes encrypted in multiple autoloaders or libraries that use the encryption kit, for example, when you install the HP MSL Library Extender with two libraries that are using the encryption kit or combine the functions of two or more autoloaders or libraries into a larger library.

To combine the keys from multiple key server tokens:

1. Select the destination token for the encryption keys and set it aside. This token needs to have enough remaining capacity for all of the keys that will be copied onto it. In most cases, this will be a new token or one with only a few keys.

   NOTE: The current encryption key is the one used to encrypt data when writing tapes. The current encryption key from this token will remain the current encryption key after the keys are combined. If this a new token, the current encryption key from the first set of keys put on the token will be the current encryption key.

   Figure 34 The first five keys were on the original token; keys 6 and 7 were added from another token

2. Verify that no backup operations are in progress.
3. Log into the RMI and supply the PIN for the token in the autoloader or library.
   - MSL6480 — Log into the RMI as the security user, navigate to **Configuration > Encryption > USB — MSL Encryption Kit** screen and then enter the PIN in the **Pin Management** section.
   - Autoloader and other libraries — Log into the RMI as the administrator user and enter the PIN in the **Configuration > Security** screen.
4. For each of the tokens other than the destination token:
   a. Insert the token into the USB port on the back of the autoloader or library.
   b. If the **Number of Keys to Backup** option is not visible or active, you must back up all keys on the token. Once all of the keys are backed up, you will be able to select the number of keys to back up.
   c. In the **Back up Token to File** pane, enter a password which will be used to secure the data file on the computer in both fields. The second one ensures that the password was typed correctly.
   d. Click **Submit Token Backup File Password**.
   e. If the **Number of Keys to Backup** option is active, select the number of keys to copy onto the new token. The highest numbered keys will be copied to the file. For example, if the token contains seven keys and you select three, keys five, six, and seven will be copied.
   f. Click **Save**. The RMI will prompt you for the location to save the file. Follow the instructions in RMI.
5. Insert the destination token into the USB port of the autoloader or library.

6. For each of the token backup files created from the other tokens:
   a. Enter the password used to create the token backup file.

      Click **Submit Token Restore File Password**.

   b. Browse to the location of the token backup file. Click **Restore**. (The Browse button will be active after the token restore file password is submitted.)

      NOTE: The key server token holds up to 100 keys. If more than 100 unique keys are found on the receiving token and in the backup file, the restore process will not be initiated. You will receive warnings when a key server token is over 90% full. You should purchase new tokens and transition to using a new token when these warnings appear. Keys can never be deleted from a key server token.

7. If you paused tape write operations at the beginning of the procedure, you can resume them.

When to obtain a new key server token

The autoloader or library will issue warnings when the key server token is 90% full. When the token reaches 90% capacity, purchase additional key server tokens.

When the token is 100% full, keep it in a secure location to use when restoring data from tapes encrypted with keys on the token.

Seeding the new key server token

When transitioning from a full token to a new token, you can copy the highest numbered keys from the full token to the new token to enable read operations from tapes written with keys on the full token. The highest numbered keys are normally the most recent.

To seed a new token:

1. Verify that no backup operations are in progress.
2. Log into the RMI.
   - MSL6480 — Log into the RMI as the security user. You will need the security user password.
   - Autoloader and other libraries — Log into the RMI as the administrator user. You will need the administrator user password.
3. Insert the full token into the USB port on the back of the autoloader or library, and enter the PIN.
4. If the **Number of Keys to Backup** option is not visible, you must back up all keys on the token before creating a file with just some of the keys.
   a. In the **Back up Token to File** pane, enter a password which will be used to secure the data file on the computer in both fields. The second one ensures that the password was typed correctly.
   b. Click **Submit Token Backup File Password**.
   c. Click **Save**. The RMI will prompt you for the location to save the file. Follow the instructions in RMI.
   d. Continue with step 5 to create a file with a subset of the keys.
5. In the **Back up Token to File** pane, enter a password which will be used to secure the data file on the computer in both fields.
6. Click **Submit Token Backup File Password**.
7. In the **Number of Keys to Backup** field, select the number of keys to copy onto the new token. The highest-numbered keys, which are normally the most recent, will be copied. For example, if the token has 100 keys and you select 3, keys 98, 99, and 100 will be copied.
8. Click **Save**. The RMI will prompt you for the location to save the file. Follow the instructions in RMI.

9. Insert the new token into the USB port of the autoloader or library.
10. Follow the RMI instructions to create a PIN for the new token.
11. Enter the password used to create the token backup file. Click **Submit Token Restore File Password**.
12. Browse to the location of the token backup file containing the seed keys. Click **Restore**. (The Browse button will be active after the token restore file password is submitted.)
13. If you paused write operations at the beginning of the procedure, you can resume them.

Restoring encrypted data during disaster recovery

When restoring encrypted data after a disaster, you will need:

- The tape cartridges containing the encrypted data.
- Depending on your token data backup process, you will need one of the following:
  - A token data backup file, with the password for the file, and a token with room for the keys on the data backup file. If the token has been initialized, you will need its PIN.
  - A token containing the encryption keys used to write the tapes and the PIN for the token. If new keys were restored to the second token as the keys were made, the second token will contain all of the keys and can be used to restore the data.
- An HP StoreEver 1/8 G2 Tape Autoloader or MSL2024, MSL4048, MSL6480, MSL8048, or MSL8096 Tape Library supported by your backup application with at least one LTO-4 or later generation tape drive.
- The security password for the MSL6480 library or the administrator password for the autoloader or other library.

The key server tokens work with any HP StoreEver 1/8 G2 Tape Autoloader or MSL2024, MSL4048,MSL6480, MSL8048, or MSL8096 Tape Library with at least one LTO-4 or later generation tape drive. If you have an autoloader or a library with an older generation tape drive, you can upgrade to an LTO-4 or later generation tape drive for the recovery operation. You may need to update the firmware in the autoloader or library and tape drive to support the encryption kit. You will need the security password for the MSL6480 library or the administrator password for the autoloader or other library.

For examples of token data backup and restore processes, see "Backing up the key server token data" (page 14).

Using the encryption kit with partitions or logical libraries

When a library with multiple LTO-4 or later generation tape drives is partitioned into multiple logical libraries, encryption can be enabled or disabled for each partition or logical library containing an LTO-4 or later generation tape drive, but all other encryption settings apply to the entire library.

Only one write key is used for all new or formatted tapes in all of the LTO-4 or later generation tape drives in the tape library.

Restoring the encryption configuration after a chassis or library controller replacement

The encryption configuration is saved when you save the autoloader or library configuration database to a file or USB flash drive. The saved configuration database will make it easier to recover the autoloader or library configuration, including the encryption configuration, if you need to replace the chassis or library controller.

Use the RMI screen for your device to save the configuration database to a file or restore it from a file. You will need the administrator user password.

- MSL6480 — **Configuration > System Save/Restore Configuration** screen
- Autoloader and other libraries — **Configuration > Save/Restore** screen

Figure 35 MSL6480 Configuration > System Save/Restore Configuration screen

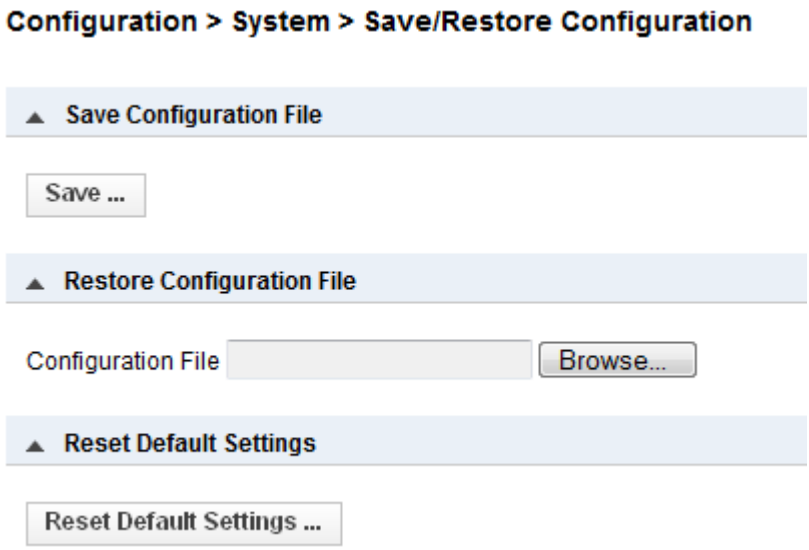
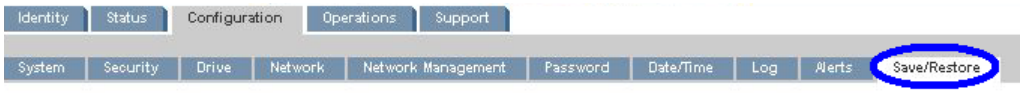


Figure 36 Autoloader and other libraries — Configuration > Save/Restore tab



NOTE: You cannot restore a saved configuration or the factory defaults while encryption is enabled. This restriction ensures that encryption cannot be disabled without a token and its PIN. Disable encryption before restoring a saved configuration or the factory defaults.

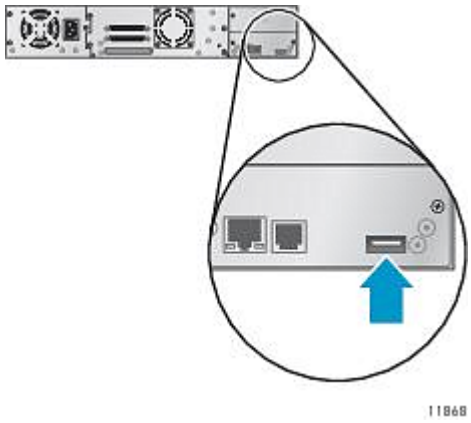
5 Troubleshooting

Installation problems

The library does not have a USB port

Some MSL2024 and MSL4048 Tape Libraries have silver tape covering the USB port. Remove the tape to locate the USB port in the location shown in Figure 37 (page 43).

Figure 37 USB port location



Operation problems

Encryption token LED

The LED on the encryption token should be lit when the token is plugged into the back of the autoloader or library when the autoloader or library is powered on.

If the LED is not lit, the token is not receiving power through the USB port. To determine whether the problem is with the token or the autoloader or library:

1. Remove and then insert the token in the autoloader or library USB port.
   - If the LED flashes for five to ten seconds and then does not light, the token may be defective. Contact your HP Service representative.
   - If the LED does not flash or light, continue to step 2.
2. Insert a good USB flash drive in the autoloader or library USB port.
   - If the good flash drive receives power, the problem could be with the token.
   - If the good flash drive does not receive power, the problem could be with the autoloader or library.
3. Insert the key server token into the USB port of a computer. The token LED will flash when the token receives power but the computer will not be able to read the contents of the token.
   - If the token LED lights or flashes, the problem could be with the autoloader or library.
   - If the token LED remains unlit, the problem could be with the token.

If the LED flashes continuously, the device into which the key server token is plugged cannot communicate with the key server token. If the key server token is plugged into the autoloader or library, verify that the autoloader or library firmware supports the encryption kit. See "Requirements for using the encryption kit" (page 6).

Troubleshooting table

You can access encryption kit features from the RMI. Accessing the RMI encryption kit screen requires a password.

Table 5 RMI encryption kit screen location, user, and password

Device	RMI screen	User	Password
MSL6480	**Configuration > Encryption > USB — MSL Encryption Kit**	Security	Security user password
Autoloader and other libraries	**Configuration > Security**	Administrator	Administrator user password

Table 6 Troubleshooting table

Problem	Cause	Solution
Both backup to and restore from an LTO-4 or later generation tape drive are not working.	The tape drive ports are disabled because encryption is enabled and the tape drive firmware does not support the encryption kit.	Use the RMI or USB flash drive to update the drive firmware to the latest version. Enable encryption after the firmware is updated. See "Tape drive and drive firmware requirements" (page 7) for minimum drive firmware revisions that support the encryption kit.
	The token does not have a key.	Create an encryption key from the RMI encryption kit screen.
	The token has not been initialized.	Set the PIN and generate a key from the RMI encryption kit screen.
	The PIN has not been entered.	Enter the PIN from the RMI encryption kit screen.
	An LTO-3 tape cartridge is being used. When encryption is enabled, an LTO-4 or later generation tape drive will neither read from nor write to an LTO-3 tape cartridge.	Use the same generation tape cartridge to write data with an LTO-4 or later generation tape drive. Disable encryption to read data from an LTO-3 tape cartridge.
Cannot write encrypted data to a tape.	The tape and/or the tape drive are not LTO-4 or later generation.	Both the tape and tape drive must be LTO-4 or a later generation to write encrypted data. When encryption is enabled, an LTO-4 or later generation tape drive will not write an LTO-3 tape.
Cannot append encrypted data to an LTO-4 tape.	Direct append operations are not supported by the application.	The application or script writing the data must read the tape header before appending data.
	The token currently installed in the autoloader or library does not have the key used to write the tape.	Insert the token with the correct write key for the tape in the autoloader or library. Suspend other write operations while the other token is installed to avoid writing new or formatted tapes with the wrong write key.
	The tape has unencrypted data on it.	Replace the tape or disable encryption while the tape is being written. The autoloader or library will not write both encrypted and unencrypted data on the same tape.
Cannot restore encrypted data from an LTO-4 or later generation tape.	The token currently installed in the autoloader or library does not have the key used to write the tape.	Insert the token with the write key for the tape in the autoloader or library. Suspend other write operations while the other token is installed to avoid

Table 6 Troubleshooting table *(continued)*

Problem	Cause	Solution
		writing new or formatted tapes with the wrong write key.
Token does not recognize the PIN.	You entered the incorrect PIN.	Find the correct PIN and enter it.
	A different token has been installed in the autoloader or library.	Check the RMI encryption kit screen to verify that the correct token is installed in the autoloader or library. Either replace the token with the correct token or enter the PIN for the currently-installed token.
Token requests a new PIN.	A new token has been installed in the autoloader or library.	Either replace the token with the correct token or initialize the new token from the RMI encryption kit screen.
Lost password to the token backup file.	The person who knew the password has forgotten it or is unavailable.	Back up the token to a different file or restore the keys from a different recent backup file with a known password.
The autoloader or library will not restore the token backup file to a token.	The number of unique keys in the token backup file and the token is greater than 100.	Check the RMI encryption kit screen to verify that the correct token is installed in the autoloader or library. Either replace the token with the correct token or restore the token backup file to a new token. Keys can never be deleted from a token.
	The receiving token has not been initialized.	Use the RMI to set the PIN.
A token backup file created on an MSL6480 cannot be restored on an autoloader or other library, or a token backup file created on an autoloader or other library cannot be restored on an MSL6480.	MSL6480 firmware versions 4.20 and earlier saved the token backup file with a different format the autoloader and other libraries.	MSL6480 firmware versions 4.30 and newer use the same file format as the autoloader and other libraries. If your token backup file has `.tkn` file suffix, only restore it on an MSL6480. **IMPORTANT:** Restoring a `.tkn` token backup file created on the MSL6480 to the HP 1/8 G2 autoloader or MSL2024, MSL4048, MSL8048, or MSL8096 library will cause the target device to become unresponsive. If this happens, power cycle the target device.
The token PIN has been lost.	The person who knew the PIN has forgotten it or is unavailable.	Restore the latest token backup file to a new token and be sure not to lose the PIN for the new token.
One or more logical libraries is not shown in the RMI encryption kit screen.	The logical library does not have an LTO-4 or later generation tape drive or the tape drive firmware does not support the encryption kit.	Configure the logical libraries and tape drives so the logical libraries that need encryption have at least one LTO-4 or later generation tape drive. Verify that the LTO-4 tape drives have a firmware revision that supports the encryption kit. See "Tape drive and drive firmware requirements" (page 7) for minimum drive firmware revisions that support the encryption kit.
The autoloader or library is unable to apply encryption settings.	The backup application disabled encryption on the tape drive.	Disable the backup application, power cycle the autoloader or library, and then try enabling encryption again in the RMI.

Table 6 Troubleshooting table *(continued)*

Problem	Cause	Solution
A PIN or backup file password longer than 15 or 16 characters is not accepted.	Some earlier versions of the RMI allowed longer passwords to be entered, but the firmware only stored the first 15 or 16 characters when encrypting the PIN or password.	Try entering just the first 15 or first 16 characters of the PIN or backup file password. If necessary, downgrade the firmware to an earlier version and then change the PIN to 15 or fewer characters. Back up the token data to a file, using a password with 15 or fewer characters. Upgrade the firmware to the newest version.
Automatic key generation is enabled but a key was not generated at the specified time.	The autoloader or library will only generate a new key if the device is powered on, the token is logged in with the token password, and all tape drives are empty.	Update either the backup schedules or key generation schedule to so that all tape drives will be empty when the key is scheduled to be generated. Ensure that the device is powered on and that the token is logged in when the key is scheduled to be generated. Generate a new key manually when one was not generated automatically.
An autoloader or MSL2024, MSL4048, MSL8048, or MSL8096 tape library becomes unresponsive when restoring a token backup file.	MSL6480 firmware 4.20 and earlier firmware versions saved the token backup file with a different format the autoloader and other libraries. When this file is restored onto an autoloader or MSL2024, MSL4048, MSL8048, or MSL8096 tape library, the device will become unresponsive.	MSL6480 firmware versions 4.30 and newer use the same file format as the autoloader and other libraries. If your token backup file has `.tkn` file suffix, only restore it on an MSL6480. **IMPORTANT:** Restoring a `.tkn` token backup file created on the MSL6480 to the HP 1/8 G2 autoloader or MSL2024, MSL4048, MSL8048, or MSL8096 library will cause the target device to become unresponsive. If this happens, power cycle the target device.

MSL6480 event codes

Table 7 Warning events

Event code	Message and description
4051	A new encryption key could not be created because media is loaded in one or more drives. Unload the media from all drives and then retry the manual key creation again.
4052	A new encryption key could not be created because media is loaded in one or more drives. Unload the media from all drives and then automatic key generation will occur during the next scheduled time frame, or generate a new token key manually.

Table 8 Informational events

Event code	Message
9017	MSL Encryption Kit password has changed.
9018	MSL Encryption Kit password has been requested.
9019	MSL Encryption Kit password has been created.
9020	MSL Encryption Kit password has been set.
9021	MSL Encryption Kit token has been initialized.
9022	MSL Encryption Kit backup has been done.

Table 8 Informational events *(continued)*

Event code	Message
9023	MSL Encryption Kit restore has been done.
9030	An invalid MSL Encryption Token was inserted.
9039	Token key creation attempt failed due to media being loaded in one or more drives.

Autoloader and other library event codes

Table 9 Error codes

Error code	Message	Cause	Solution
E1	Key server token backup not successful — not enough space is available on the token.	A key server token restore process was attempted but the receiving token did not have enough room for the keys in the token backup file.	Restore the token backup file to a token with enough space for the keys on the token and the keys in the token backup file.
E3	Error during key server token backup; the backup process was not successful.		• Retry the restore process with a different token. • Make a new token backup file and retry the restore process with the new backup file. • Contact HP Service.
E4	Drive firmware does not support encryption.	An attempt was made to enable encryption with a version of tape drive firmware that does not support native encryption.	Verify that you have the correct tape drive firmware version installed. See "Tape drive and drive firmware requirements" (page 7) for minimum drive firmware revisions that support the encryption kit.
E5	Drive generation does not support encryption.	An attempt was made to enable encryption with a tape drive that does not support native encryption.	Only enable encryption on LTO-4 or later generation tape drives.

Table 10 Warning events and messages

Code	Message	Cause	Solution
51	Incompatible medium	The LTO-4 or later generation tape drive is trying to read or write an LTO-3 or earlier generation tape while encryption is enabled.	Only use the same generation tape in an LTO-4 or later generation tape drive when encryption is enabled. An LTO-4 or later generation tape drive will not read or write LTO-3 tape cartridges when encryption is enabled.
56	No decryption key available on token	The key needed to restore a decrypted tape is not available on the token currently installed in the autoloader or library.	Insert the token with the key used to encrypt the key into the autoloader or library and retry the restore operation.
57	Key server token PIN required	The autoloader or library needs the PIN to access the data on the token.	Enter the PIN from the RMI **Configuration > Security** screen.
5A	Unable to downgrade firmware while encryption enabled.	An attempt was made to load tape drive firmware that does not support the encryption kit on an	Either upgrade the tape drive firmware to a version that supports the encryption kit or disable encryption. Do not enable

Table 10 Warning events and messages *(continued)*

Code	Message	Cause	Solution
		LTO-4 tape drive while encryption is enabled.	encryption until tape drive has firmware that supports the encryption kit. See "Tape drive and drive firmware requirements" (page 7).

6 Support and other resources

Contacting HP

Before you contact HP

Be sure to have the following information available before you contact HP:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

HP contact information

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/e-updates

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to **storagedocsFeedback@hp.com**. All submissions become the property of HP.

Related information

Documents

- *HP StoreEver 1/8 G2 Tape Autoloader User and Service Guide*
- *HP StoreEver MSL2024, MSL4048, MSL8048, and MSL8096 Tape Libraries User and Service Guide*
- *HP StoreEver MSL6480 Tape Library User and Service Guide*

You can find these documents from the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

In the Storage section, click **Tape Storage and Media** and then select your product.

Websites

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/manuals

- http://www.hp.com/support/downloads
- http://www.hp.com/support/mslg3stree — Troubleshooting tree
- http://www.hp.com/go/tapetools — HP Library and Tape Tools

Document conventions and symbols

Table 11 Document conventions

Convention	Element
Blue text: Table 11 (page 50)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

WARNING! Indicates that failure to follow directions could result in bodily harm or death.

CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Customer self repair

HP CSR programs allow you to repair your storage product. If a CSR part needs replacing, HP ships the part directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your HP-authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider, or see the CSR website:

http://www.hp.com/go/selfrepair

This product has no customer replaceable components.

Index

A
automatic key generation, 14

B
backing up the token data, 34
backup process
  token data, 14

C
conventions
  document, 50
  text symbols, 50
current key, 9
customer self repair, 50

D
disaster recovery, 41
document
  conventions, 50
  related documentation, 49
documentation
  HP website, 49
  providing feedback, 49

E
encryption
  enabling or disabling, 33

F
firmware requirements
  autoloader or library, 7
  tape drive, 7

G
generating a new encryption key, 32

H
help
  obtaining, 49
HP
  technical support, 49

I
installation
  backing up the initial key, 28
  configuring encryption
    autoloader and other libraries, 25
    MSL6480, 20
  identifying product components, 18
  preparing key server tokens, 19
  preparing the autoloader or library, 18

L
LED, 8
  troubleshooting, 43
logical libraries, 41

P
PIN, 16
  changing, 31
  entering, 30
  power cycle, 31
power loss, 17

R
related documentation, 49
restoring encrypted data, 38
restoring the encryption configuration, 41
restoring the token data, 36
RMI
  encryption kit screen, 44

S
Subscriber's Choice, HP, 49
symbols in text, 50

T
technical support
  HP, 49
  service locator website, 49
text symbols, 50
token data backup process, 14
token naming, 16
troubleshooting
  error codes
    autoloader and other libraries, 47
  event codes
    autoloader and other libraries, 47
    MSL6480, 46
  informational events
    MSL6480, 47
  LED, 43
  no USB port, 43
  troubleshooting table, 44
  warning events
    autoloader and other libraries, 48
    MSL6480, 46

U
USB port, 8

W
websites
  customer self repair, 50
  HP , 49
  HP Subscriber's Choice for Business, 49
  product manuals, 49